IN THE CLAIMS:

The text of all pending claims (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with <u>underlining</u> and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

Please AMEND claims 1-8, and ADD claims 9-11, in accordance with the following:

1. (CURRENTLY AMENDED) A method for determining whether or not electronic mail transmitted through a network is infected by a mail virus, said method comprising ~~the steps of~~:

<u>registering a second address as a receiver address in an address table for mail virus detection;</u>

~~(a)~~ determining whether ~~or not~~ a first address indicated by <u>an</u>~~the~~ electronic mail transmitted <u>from a client</u> through the network indicates <u>the</u>~~a~~ second address recorded in <u>the</u>~~an~~ address table for mail virus detection<u>, the first address being registered in an address book of the client;</u>~~to receive the mail virus, instead of receiving a regular electronic mail,~~

~~(b)~~ storing information concerning the electronic mail as mail virus information <u>in</u>~~into~~ <u>a</u> mail virus information table <u>in response to</u>~~when~~ the first address of the electronic mail <u>indicating</u>~~indicates~~ the second address; and

~~(c)~~ suppressing <u>transmission of</u>~~sending~~ <u>any</u>~~other~~ electronic mail~~, the electronic mail~~ <u>that includes</u>~~including~~ the mail virus~~ information~~.

2. (CURRENTLY AMENDED) The method as claimed in claim 1, further comprising ~~a step of (c)~~ reporting a mail virus detection~~ based on the determination in said step (a)~~ to at least one predetermined report address <u>in response to the first address indicating the second address</u>.

3. (CURRENTLY AMENDED) The method as claimed in claim 1, further comprising ~~the steps of~~:

~~(d)~~ compressing the electronic mail <u>having the first address indicating the second address</u>~~detected in said step (a)~~; and

~~(e)~~ attaching the <u>compressed</u> electronic mail~~ compressed in said step (d)~~ to a report electronic mail for reporting the mail virus detection, <u>and reporting the mail virus detection by</u>

sending the report electronic mail to at least one predetermined address.~~wherein a step (c) reports the mail virus detection by sending the report electronic mail attaching the electronic mail compressed in said step (d).~~

4.   (CURRENTLY AMENDED) A computer-readable recording medium recorded with program code for causing a computer to determine whether or not electronic mail transmitted through a network is infected by a mail virus, said computer-readable recording medium comprising codes for:

registering a second address as a receiver address in an address table for mail virus detection;

~~(a)~~ determining whether ~~or not~~ a first address indicated by an~~the~~ electronic mail transmitted from a client through the network indicates~~is the same as~~ the~~a~~ second address recorded in the address table for mail virus detection, the first address being registered in an address book of the client;~~, and~~

storing information concerning the electronic mail as mail virus information in a mail virus information table in response to the first address of the electronic mail indicating the second address; and

~~(b)~~ suppressing transmission of any~~sending other~~ electronic mail that includes the mail virus.~~of a same type as the electronic mail when said step (a) determines that the electronic mail indicates the second address for the mail virus detection.~~

5.   (CURRENTLY AMENDED) The computer-readable recording medium as claimed in claim 4, further comprising~~a~~ code for ~~(c)~~ reporting a mail virus detection ~~based on the electronic mail detected in said code (a)~~ to at least one predetermined report address in response to the first address indicating the second address.

6.   (CURRENTLY AMENDED) The computer-readable recording medium as claimed in claim 5, further comprising ~~the~~ code for:

~~(d)~~ compressing the electronic mail having the first address indicating the second address~~detected in said code (a)~~; and

~~(e)~~ attaching the compressed electronic mail ~~compressed in said code (d)~~ to a report electronic mail for reporting the mail virus detection, and reporting the mail virus detection by sending the report electronic mail to at least one predetermined address.~~wherein said code (c)~~

~~reports the mail virus detection by sending the report electronic mail attaching the electronic mail compressed in said code (d).~~

7. (CURRENTLY AMENDED) A method for detecting electronic mail infected by a ~~mail~~ virus, the method comprising:

detecting an electronic mail as being infected by a virus in response to determining that a first address of an electronic mail transmitted from a client corresponds to a second address recorded in an address table for virus detection, the first address being registered in an address book of the client~~comparing a first type of a first piece of electronic mail to a second type of a second piece of electronic mail~~; and

suppressing transmission of the electronic mail. ~~a transmission of said second piece of electronic mail if said second type is substantially equivalent to said first type and an address of said first piece of electronic mail is an address for mail virus detection.~~

8. (CURRENTLY AMENDED) The method as claimed in claim 1, wherein the mail virus information indicates one or more~~at least one of~~ values of a sender electronic mail address, a data size, a title, or a combination thereof, which are shown in the electronic mail indicating the second address.

9. (NEW) The method of claim 7, further comprising storing information corresponding to the electronic mail as virus information in a virus information table in response to detecting the electronic mail as being infected by the virus.

10. (NEW) The method of claim 7, further comprising suppressing transmission of any electronic mail that includes the virus in response to detecting the electronic mail as being infected by the virus.

11. (NEW) The method of claim 7, further comprising reporting the virus detection to at least one predetermined report address in response to detecting the electronic mail as being infected by the virus.